ABSTRACT

A system for updating a communications key(s) performs an authentication(s) of the unit and/or of the communications system using an update key. By using the update key to perform the authentication(s), the key update system can reduce communications between a home communications system and a visiting communications system by sending the update key to the visiting communications system while maintaining the communications key at the home communication system. For example, in performing a key update, the home communications system generates a communications key, such as a new authentication key SSD-A-NEW, using a sequence RANDSSD generated at the home communications system and a secret key A-KEY maintained at the home communications system and at the unit. The home communications system generates the update key SSD-KEY also using the sequence RANDSSD and the secret key A-KEY. The home communications system sends the update key SSD-KEY and the sequence RANDSSD to the visiting communications system, and the visiting communications system sends the sequence RANDSSD to the unit. The unit generates the new communications key, such as the new authentication key SSD-A-NEW, and the update key SSD-KEY in the same manner as the home communications system. Because the visiting communications system has the update key SSD-KEY, the visiting authentication system can generate the signature value(s) AUTHSSD and/or AUTHBS using the update key at the visiting communications system to authenticate the unit and/or the communications system.